Folkekirkens It's arkitekturprincipper

Arkitekturprincipperne består af 11 principper, som skal anvendes ved alle nyanskaffelser og større ændringer af eksisterende it-systemer.

Arkitekturprincipperne skal sikre, at ændringer og nyanskaffelser sker i henhold til den fælles it-arkitektur, så der sikres en fælles ramme for alle it-tiltag.

Principperne skal anvendes ud fra et følg-eller-forklar-princip. I udgangspunktet skal alle tiltag leve op til de krav som de enkelte principper stiller, med mindre der er klare behov for at afvige. I så fald skal det klart beskrives hvordan der afviges fra principperne, og hvad de positive og negative konsekvenser ved dette vil være. Afvigelserne skal godkendes af de ansvarlige for det konkrete tiltag.

1. BEHOV FOR IT-UNDERSTØTTELSE VURDERES I FORHOLD TIL EKSISTERENDE SYSTEMER

Definition

Ved behov for ny eller forbedret it-understøttelse vurderes dette altid i forhold de eksisterende centrale og lokale it-løsningers funktionalitet, brugerflader og integrationsmuligheder.

Begrundelse

Vi ønsker at udnytte de it-løsninger vi har mest muligt, fremfor at købe nyt. Samtidig ønsker vi at sikre størst mulig genanvendelighed i de nye løsninger, for løbende at skabe et fleksibelt, sammenhængende og ensartet miljø. Dette muliggør, at Folkekirkens og ministeriets opgaver i stadig stigende grad kan løses mere sammenhængende og samtidig lette drift, administration og vedligehold af løsningerne.

Konsekvens

Ved identifikationen af nye eller ændrede behov vurderes:

- Hvilken funktionalitet der ønskes til at imødekomme behovet?
- I hvilken grad funktionaliteten eller dele af funktionaliteten findes i de eksisterende applikationer og services?
- Det tilstræbes at nye løsninger er opbygget i moduler da dette giver mindre kompleksitet.
- Modulopbygning letter testarbejdet ved ændringer da der ikke er så stor afhængighed til den samlede løsning.

Dette betyder, at:

Ved udarbejdelse af projektoplæg skal det beskrives hvilken funktionalitet der findes i eksisterende moduler.
Hvis der sker genanvendelse af eksisterende moduler, bør det sikres at modulerne er tidssvarende, både teknisk og ift. brugeren. Det skal vurderes om videreudvikling eller nyudvikling vil være mest fordelagtigt.

Ved nyudvikling opbygges applikationer i moduler, der skaber størst mulig konfigurerbarhed og muliggør genanvendelse.

2. ANVEND STANDARDSYSTEMER OG -PLATFORME

Definition

Ved behov for funktionalitet foretrækker vi at basere os på anerkendte og udbredte løsninger. Hvis det ikke er muligt, skal udvikling baseres på anerkendte og udbredte udviklingsværktøjer.

Begrundelse

Vi ønsker at sikre et robust og ensartet miljø. Dette gøres ved i størst muligt omfang at basere os på velafprøvet teknologi og anvendelse af platforme, der muliggør ensartethed på tværs af løsningerne. Samtidig vil det lette drift, administration og vedligehold af løsningerne.

Konsekvens

Ved anskaffelser foretrækkes anerkendte og udbredte løsninger. Når disse ikke kan opfylde de væsentligste behov, så udvikling er påkrævet, anvendes anerkendte og udbredte udviklingsværktøjer til levering af nye services og applikationer.

Dette betyder, at:

Ved anskaffelser stilles krav om, at anerkendte og udbredte løsninger foretrækkes. Når udvikling er nødvendig anvendes anerkendte og udbredte udviklingsværktøjer.

3. UDNYT DEN FÆLLESOFFENTLIGE INFRASTRUKTUR

Definition

Vi udnytter den fælles offentlige infrastruktur til at sikre en effektiv understøttelse af brugerne og borgere, og vi lever op til de fællesoffentlige krav om digitalisering.

Begrundelse

Ved at anvende fælles kilder og komponenter undgår vi at skulle egenudvikle komponenter på de relevante områder. Anvendelse af fælles datakilder sikrer samtidigt at vi ikke skal vedligeholde og opbevare data der er tilgængelige ved fælles kilder.

Anvendelsen af fællesoffentlige komponenter (fx NemID, Digital Post) giver størst mulig genkendelighed for brugerne.

Ved at genbruge og udnytte eksisterende offentlig infrastruktur spares ressourcer på nyudvikling og vedligehold.

Vi skal leve op til fællesoffentlige krav vedr. digitalisering.

Konsekvens

Den fælles offentlige infrastruktur, både data og fælleskomponenter, skal anvendes i størst muligt omfang.

Ved udvikling af nye systemer eller væsentlige ændringer i eksisterende systemer skal det undersøges, hvilke fællesoffentlige data eller komponenter der kan indgå i løsningen.

Dette betyder, at:

Ved anskaffelse eller udvikling af nye løsninger, skal der stilles krav om anvendelse af de fællesoffentlige løsninger og infrastrukturkomponenter, herunder NemKonto, NemID, NemLog-In, Digital Post, CPR, CVR.

4. DEN ANVENDTE SIKKERHEDSMODEL TILPASSES DATAS KATEGORISERING

Definition

Vi anvender en differentieret sikkerhedsmodel som understøtter den passende sikkerhedsniveau for den konkrete løsning, og balancerer behovet for henholdsvis fleksibel og sikker adgang til applikationer og services på tværs af platforme.

Begrundelse [UBK1]

Vi vil sikre at der anvendes passende sikkerhedsforanstaltninger til den enkelte løsning.

For at kunne understøtte ændret brugeradfærd med anvendelse af applikationer og services på tværs af platforme og deraf øget behov for udveksling af data anvendes en differentieret sikkerhedsmodel.

Da datas integritet og tilgængelighed altid er vigtigt, sikres dette uanset sikkerhedsmodel.

Konsekvens

Sikkerhedskrav tilpasses de data der behandles i det enkelte system, service og applikation.

Ved behov for ny eller forbedret it-understøttelse gennemføres en vurdering af data i løsningen, hvilket bestemmer niveauet for datasikkerheden, som behandles jf. nedenstående datakategorier

Højere sikkerhed		Lavere sikkerhed
Ministerbetjening Personregistrering	Sagsbehandling Journalisering Løn- og personale-administration Bogføring Økonomistyring	Generelle dokumenter, regneark og præsentationer m.m. E-mails og sms Generel information

Det skal sikres, at enhver service eller applikation kan overholde det valgte sikkerhedsniveau.

Dette betyder, at:

I starten af ethvert projekt laves en vurdering af data i løsningen. Resultatet af vurderingen indarbejdes i projekt set-up'et.

Den systemansvarlige foretager regelmæssigt(baseret på risikobilledet) en vurdering af, om det sikkerhedsmæssige niveau for det enkelte system, service eller applikation er passende.

5. ALTID FOKUS PÅ DATASIKKERHED

Definition

Vi har gennem hele en applikations eller services livscyklus fokus på at sikre den krævede datasikkerhed.

Begrundelse

Opretholdelse af et tilstrækkeligt niveau for datasikkerhed for at hindre misbrug er afgørende for at overholde gældende lovgivning og sikre tillid til de it-services, som vi leverer således, at vi er forberedte til at efterleve nye krav ved lovgivning eller regulering, fx via persondataforordningen.

Konsekvens

Ved større ændringer i en service eller applikation sikres, at kun nødvendige data indsamles, og kategorien af disse data vurderes. Der skal samtidig altid gennemføres specifik risikovurdering for det enkelte projekt.

På baggrund af datas kategori og risikovurderingen vælges det rette niveau for beskyttelse af data. Desuden fastlægges:

- Hvilke sikkerhedszoner som kan anvendes?
- Hvilket sikkerhedsniveau for kommunikation og evt. kryptering af data der kræves?
- Hvilke krav der skal stilles til adgangskontrol?
- Hvilket niveau af sporbarhed, fx i form af logning, der behøves?

Den systemansvarlige foretager regelmæssigt opfølgning på hvilke data, der anvendes i systemet og vurderer på baggrund heraf, om systemet lever op til de nødvendige datasikkerhedsmæssige krav.

Dette betyder, at:

I starten af ethvert projekt laves en risikovurdering vurdering af løsningen. Resultatet af vurderingen indarbejdes i projekt set-up'et.

Ved indgåelse af aftaler med leverandører der håndterer personhenførbare data, indgås Databehandleraftale.

En gang om året går de systemansvarlige alle systemer igennem, herunder eksterne for at se om de er klassificeret rigtigt i forhold til om der er fortrolige data på systemet.

Hver 1 år sikrer Folkekirkens It at der laves scanning af alle systemer og services der er tilgængelige uden for Kirkenettet.

Alle eksterne leverandører skal gennemgås for valid databehandleraftale hvert år.

Alle leverandører skal tiltræde Governance i Kirkenettet

6. ANVEND FÆLLES DATAMODEL

Definition

Vi anvender vores fælles datamodel for at sikre ajourførte og konsistente masterdata på tværs af alle applikationer og services.

Begrundelse

Ved at sikre ajourførte og konsistente masterdata på tværs af alle applikationer og services, sikres det, at brugere altid har adgang til den korrekte information. Samtidigt tydeliggør den fælles datamodel, hvor masterdata er placeret og dermed, hvor data fødes, samt hvem der har til ansvar at sikre opdatering af data.

Konsekvens

Den fælles datamodels rammer for indhold og ansvar skal overholdes ved al udvikling af nye systemer eller væsentlige ændringer.

Nye løsninger må ikke rumme proprietære masterdata, der allerede findes et andet sted.

Dette betyder, at:

Folkekirkens It's krav til anvendelse af masterdata skal overholdes..

Ved anskaffelse og udvikling skal datamodellen anvendes så nye applikationer og services overholder krav til anvendelse og vedligehold af masterdata.

Ved anskaffelse og udvikling af nye applikationer og services skal datamodellen opdateres, og evt. ændringer skal godkendes af de ansvarlige for den fælles datamodel.

7. FOKUS PÅ BRUGERVENLIGHED

Definition

Vi har altid fokus på at sikre høj brugervenlighed i vores løsninger ved at sikre brugerinvolvering og udvikle brugerflader målrettet den enkelte bruger og sikre sammenhæng og ensartethed på tværs af vores løsninger.

Begrundelse

Brugerinddragelse giver bedre løsninger slutbrugerne ved løbende at anvende deres viden og respons i it-projekterne.

Fokus på optimalt design af brugergrænsefladen vil sikre brugeren af systemet en væsentlig bedre oplevelse. For den enkelte bruger vil enkle og ensartede brugerflader på tværs af systemerne betyde mindre oplæring, en lettere arbejdssituation og større effektivitet. Særlig for brugere med begrænset anvendelse er enkelhed og overskuelighed afgørende.

Et brugervenligt design vil give færre kilder til fejl ved brug af systemet. Brugergrænsefladen er en mindst lige så væsentlig del af it-systemer som selve kodningen.

Konsekvens

Ved udvikling af nye systemer eller væsentlige ændringer i eksisterende systemer skal det sikres, at brugergrænsefladen får en optimal udformning. Dette sker ved at sikre løbende brugerinddragelse, og ved at overholde de fælles rammer, der eksisterer for brugervenlighed ved Folkekirken It.

Dette betyder, at:

Brugere skal altid inddrages i behovsafklaring og design af løsninger.

For alle websteder og selvbetjeningsløsninger skal Digitaliseringsstyrelsens proceskrav til *God selvbetjening* anvendes efter følg eller forklar-princippet. For øvrige projekter er de til inspiration.

Kravene til god selvbetjening findes her: http://arkitekturguiden.digitaliser.dk/godselvbetjening

Alt udvikles som udgangspunkt til web.

8. UNDERSTØT PLATFORMSUAFGÆNGIGHED

Definition

Vi foretrækker platformsuafhængige applikationer og løsninger på såvel pc/Mac, tablets og smartphones, inden for de it-sikkerhedsmæssige rammer. Hvis dette ikke er muligt, skal applikationer og services være tilgængelige på de gængse platforme og i det omfang, det er relevant for brugerne.

Begrundelse

Vi ønsker at understøtte brugernes behov for adgang til it-understøttelse på de enheder, hvor de finder det fordelagtigt og med den funktionalitet der er relevant, og dermed tilbyde en mere fleksibel adgang til it-løsningerne.

Konsekvens

Ved udvikling eller anskaffelse af nye applikationer eller services skal det kortlægges, hvilke brugerbehov der er ift. it-understøttelse på forskellige typer af enheder.

Der foretrækkes applikationer og services, som kan gøres tilgængelige for brugerne på alle gængse platforme.

Dette betyder, at:

Ved nyudvikling og anskaffelser har vi en præference for systemer, der har en platformsuafhængig brugergrænseflade. Vi vurderer at webbaserede og responsive brugerflader giver den største platformsuafhængighed.

Ved nyudvikling og anskaffelser skal det tydeligt beskrives, hvilken funktionalitet der er tilgængelig og reelt anvendelig på de brugerflader der tilbydes de forskellige enhedstyper, herunder pc/mac, tablet, smartphone.

For hvert projekt specificeres en konkret liste over de browsere (inkl. mobil-browser) der skal understøttes. Som udgangspunkt understøller vi på PC og mac altid IE i de to sidste versioner, Edge i den nyeste version, Chrome, Safari og Firefox i den nyeste version.

9. MAKSIMAL ÅBENHED I APPLIKATIONERNE

Definition

Vi anvender åbne standarder og adgang til data i vores applikationer via velbeskrevne snitflader.

Begrundelse

Ved at anvende åbne standarder til kommunikation mellem vores applikationer og sikre adgang til alle data i den enkelte applikation via velbeskrevne snitflader sikres størst mulig fleksibilitet i udviklingen af it-understøttelsen, og risikoen for afhængighed til leverandører eller proprietære standarder mindskes.

Konsekvens

Ved alle nyanskaffelser stilles klare krav til fri adgang til alle data i applikationen via velbeskrevne snitflader og at snitflader og integrationer baseres på åbne standarder, således at vi sikrer maksimal fleksibilitet i forhold til den fremtidige udvikling af vore services

Dette betyder, at:

Ved anskaffelse og udvikling stilles krav til fri og ubegrænset adgang til alle data i applikationen via velbeskrevne snitflader.

Ved anskaffelse og udvikling stilles krav om, at snitflader og integrationer baseres på åbne standarder. Vi benytter grænseflader baseret på REST og SOAP.

10. FÆLLES SINGLE-SIGN-ON OG BRUGERADMINISTRATION

Definition

Vi anvender fælles single-sign-on og brugeradministration for alle applikationer.

Begrundelse

Det er afgørende for brugerne at skulle logge ind færrest mulige gange. For at sikre størst mulig effektivitet for brugerne er det målsætningen, at alle kun skal signe ind én gang på den samme enhed.

Fælles brugeradministration gør det mere sikkert og effektivt at administrere de mange tusinde brugere af Folkekirkens og ministeriets systemer.

Konsekvens

Folkekirkens It stiller en service til rådighed for interne og eksterne leverandører som gør det nemt at implementere ud fra gængse standarder.

Alle nye applikationer og services skal kunne anvende den fælles single-sign-on og fælles brugeradministration.

Dette betyder, at:

Ved anskaffelse og udvikling stilles krav om anvendelse af Folkekirkens It's service for at sikre understøttelse af single-sign-on.

11. PERFORMANCEKRAV TIL ALLE SERVICES OG APPLIKATIONER

Definition

Folkekirkens It opstiller individuelle performancekrav til alle sine services og applikationer.

Performancekravene som beskrives er:

- Svartid: Fra brugeren aktiverer funktionen til resultatet er tilgængeligt for brugeren.
- Driftstid: Det tidsrum på døgnet, hvor servicen eller applikationen er tilgængelig.
- Oppetid: Den procentdel af åbningstiden, hvor servicen skal svare, og den andel af klienterne, som dette skal gælde for.
- Retableringstid: Den tid, der må gå, inden servicen eller systemet fungerer igen i tilfælde af nedbrud (katastrofe).

Begrundelse

Anvendelse af performancekrav sikrer forventningsafstemning mellem it-leverandører og it-brugere om vigtigheden af den enkelte service eller applikation set i forhold til omkostningerne ved at levere den valgte performance.

Dette er for at sikre dels at applikationerne fungerer tilfredsstillende i den daglige drift, dels at der er taget højde for retableringstiden jf. den overordnede risikoanalyse for Kirkenettet.

Konsekvens

Folkekirkens It's krav for enhver service eller applikation skal overholdes. Krav vedrørende svartider, driftstid (tilgængelighed) og retableringstid skal leve op til risikovurderingen.

Det aftales, hvordan der måles og rapporteres på de valgte performancekrav.

Dette betyder, at:

- Baseret på en vurdering af den enkelte applikation eller service defineres kravene til: Svartid, Driftstid, Oppetid og Retableringstid.
- For alle applikationer og services, både internt og eksternt drevne, fastlægges det hvordan måling vil finde sted, og hvordan og med hvilket interval rapportering skal finde sted.